UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

Francisca Sandoval, Ines Hernandez,
Miriam Pachecho, Eva Reyes,
Arminda Gomez, Nidia Guerrrero,
Lucila Marquez, Maria Perez,
Azucena Garcia, Estela Laureano,
And Marlene Giron,

Court File No. 06-CV-01772(RHK/JSM)

Plaintiffs,

**AFFIDAVIT OF
MARK LANTERMAN**

v.

American Building Maintenance Industries,
Inc., a/k/a ABM Industries Incorporated
d/b/a ABM Janitorial Services, and
American Building Maintenance Co.
of Kentucky,

Defendants.

Mark Lanterman, being duly sworn, states as follows:

1. My name is Mark Lanterman. I am the Chief Technology Officer for Computer Forensic Services, Inc. located in Minnetonka, Minnesota. Our firm specializes in the forensic examination of computer data in conjunction with law enforcement agencies and law firms. Prior to joining CFS, I was a criminal investigator with over eleven years of law enforcement experience. During my last three years in law enforcement I was assigned to the United States Secret Service Electronic Crimes Task Force as its senior computer forensic analyst.

2. In connection with my current and former employment, I have supervised or participated in dozens of search warrant executions for digitally stored (computerized) records and evidence. I am certified by the United States Department of Homeland Security as a "Seized

Computer Evidence Recovery Specialist", as well as being certified in computer forensics by the National White Collar Crime Center and the International Information Systems Forensics Association. I have conducted seminars and training for the United States Secret Service, the Minnesota State Bar Association, the Hennepin County Bar Association, the International Association of Chiefs of Police, the Federal Bureau of Investigation, the New York State Bar, the California State Bar, the Wisconsin State Bar, Glasser LegalWorks and the Minnesota Institute for Legal Education. I have also testified as an expert in numerous criminal and civil legal proceedings, in both federal and state courts. Attached is my CV describing in more detail my qualifications and experience.

3. I have been retained as a court appointed neutral computer forensic analyst to the Honorable District Judge Patricia Kerr-Karasov (Hennepin County, MN) and the Honorable A.P. Fuller (Pennington County Seventh Judicial Circuit, SD)

4. Some of my representative cases include: Pioneer Press v. Star Tribune; Afremov v. AGA Medical; ING v. KMG America; Roberts v. Canadian Pacific Railroad (Minot train derailment).

5. Jacqueline Mrachek of the Greene Espel firm has previously retained me on a sexual harassment civil matter.

6. The firm of Miller and O'Brien has retained me in this case.

7. I have reviewed several deposition transcripts in this case and it is my understanding that electronic communications are used by employees of American Building Maintenance Industries, Inc. to discuss internal matters including employment policies, trainings, complaints, investigations and corrective actions which may be pertinent to Plaintiffs' case.

8. I have had an opportunity to review the deposition transcripts of Julie Mork, Charles Ketchum, Robert Janacek, Jeff Southard and Dan MacDonald. It is apparent from the transcripts that Mork, Ketchum, Southard, Jacacek and MacDonald possess neither the experience nor the training necessary to conduct a comprehensive search for electronic files relevant to this litigation.

9. The creation of a "drive image" is recognized by the computer forensic community as the proper way to preserve original electronic evidence.

10. In order to explain the importance of drive imaging, I need to briefly clarify the difference between hard drive imaging and making an electronic copy of individual files. When a computer file is saved to a storage disk, it is saved in randomly scattered sectors on the disk rather than in contiguous, consolidated blocks; when the file is retrieved, the scattered pieces are reassembled from the disk in the computer's memory and presented as a single file. Imaging the disk copies the entire disk exactly as it is, including all the scattered pieces of various files (as well as other data such as deleted file fragments). The image allows a computer forensic analyst to recreate (or "mount") the entire storage disk and have an exact copy just like the original. In contrast, a file-by-file copy (also known as a "logical file copy") merely creates a copy of an individual file by reassembling and then copying the scattered sectors of data associated with the particular file.

11. It is also important to understand that when a user "deletes" files, the files are not necessarily unrecoverable. Until the file is "overwritten" by another file, the "deleted" file is still subject to being recovered. As such, it is essential to preserve all involved computer hard drives as soon as possible since deleted, but relevant, data may be overwritten and destroyed.

12. I have designed the following protocol to be used in the production of the relevant data:

(a) First, all computers and storage media containing relevant data would be sent directly to me for imaging in the manner described above. In the event that a system or storage media cannot be sent to me, I would arrange to make the required images on site.

(b) Second, the hard drives and computers would be returned to Defendants' attorneys as soon as possible so as to avoid undue disruption to the Defendants.

(c) Third, I would prepare, from the imaged drives and a list of search terms provided by Plaintiffs, a file detail log to be provided to both Defendants and Plaintiffs. The log would list each relevant document on the hard drive with the document's file name; file extension (i.e., whether the document is a word document or power point presentation); whether the file has been deleted; the date and time when the file was created, last accessed, and last altered; the size of the file; and the location on the hard drive.

(d) Fourth, I would provide the Defendants' counsel a copy of all documents containing one or more search terms from the individual drives, so that they have the opportunity to assert privilege or non-responsiveness.

13. In order to locate pertinent information such as that referred to in Ms. Mork's deposition, it is necessary for me to conduct an examination of all devices containing data related to this matter, using the procedure I describe above. This would include the workstations of any employees who have communicated about this matter, the email server if one exists, the file server if one exists, and any other workstation or server which may contain data which is

pertinent to this case. This would be the only way to independently verify or refute the veracity of Defendants assertions they have produced all responsive records.

Further Affiant sayeth not.

Mark Lanterman

Subscribed and sworn to before me this
6TH day of JUNE, 2007.

Notary Public

MARK W. LEDBETTER
NOTARY PUBLIC - MINNESOTA
My Commission Expires Jan. 31, 2011